UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,813	06/05/2001	Ronald Mraz	YOR920010390US1	5934

35526 7590 06/03/2005

DUKE. W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/874,813	**Applicant(s)** MRAZ, RONALD	
	Examiner Paula W. Klimach	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 03/21/2005. Applicant amended Claims 1, 4, 16-17, 19, 22, 34-35, 38, 41, 48, and 54. The amendment filed on 03/21/2005 have been entered and made of record. Therefore, presently pending claims are 1-56.

Response to Arguments

Applicant's arguments filed 03/21/2005 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that there is no motivation to combine Matsumoto's encryption/decryption server with Jardin's system, which already fully provides encryption and decryption functionality. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the knowledge is generally available to one of ordinary skill in the art.

The applicant argues further that there would have been no motivation to include the teachings of Matsumoto with the teachings of Jardin, as the encryption/decryption provided by Matsumoto's server is not secure or trustworthy. The applicant cites the title, "Speeding UP Secret Computation with Insecure Auxiliary Device." However the examiner cites the same title with emphasis on Speeding Up *Secret Computation* with Insecure Auxiliary Device. Therefore the computation are still secret even if the auxiliary device is insecure. The applicant cited further the abstract on page 497. The examiner cites the same abstract the discloses, "...a smart card can efficiently *execute secret computations*..." Therefore, the auxiliary device executes secret computations. The applicant cites further paragraphs 1 and 2 on page 498. This is also not persuasive because the same paragraph says, "How a client can securely accelerate secret computations by using untrustworthy servers? This is the problem to be solved in this paper." Therefore the server may not be trusted by it is able to execute secret computations.

The applicant argues further that none of the cited references teach or suggest utilizing one engine (an online crypto engine) to perform encryption or decryption using cryptographic parameters established by another engine. This is not found persuasive. As disclosed by the applicant in the amendment (03/02/05), "Jardin already possesses processing blocks and associated functionality to perform encryption and decryption." Therefore the parameters attained during the handshake are used during encryption and decryption. The server of Matsumoto adds the computation power that may not be available at the handshake engine. Therefore the combination of Jardin and Matsumoto would result in a handshake engine that would have the extra computation power of Matsumoto.

The examiner asserts that Jardin and Matsumoto do teach or suggest the subject matter broadly recited in independent Claims 1, 19, and 38. Dependent Claims 2-18, 20-37, and 39-56 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1-56 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin (6,681,327) in view of Matsumoto et al (cited by applicant on IDS 12/2/04).

In reference to claims 1, 19, and 38, Jardin discloses a method of servicing secure transactions in a network, comprising: establishing cryptographic parameters in a handshake engine (column 4 lines 35-58); servicing a transaction in a transaction server using unencrypted data (column 8 lines 5-17); wherein the system of Jardin decrypts the client packets before fulfilling the client request.

Although Jardin discloses the decryption and encryption of communication packets between the server and the client (Fig. 3 steps 330-338) the encryption and decrption performed with the parameters established by the handshake engine (Fig. 4), Jardin does not disclose an inline crypto engine performing the earlier mentioned encryption and decryption.

Matsumoto discloses a system wherein a server, inline crypto engine performs the function of the secret computation, encryption and decryption, on behalf of a client device; therefore the inline crypto engine having capability for performing at least one of encryption and decryption of data (page 497, Introduction, paragraph 3). Since Matsumoto performs encryption and decryption then it follows that Matsumoto has the capability of performing at least one of encryption and decryption.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the trustworthy server and delegate the encryption and decryption calculations to a separate server as in Matsumoto in the broker and server system of Jardin. One of ordinary skill in the art would have been motivated to do this because the system is a trusted network wherein the computing power of an auxiliary device may be implemented.

In reference to claims 2, 20, and 39, Jardin discloses a system wherein the packets from the client are decrypted to provide unencrypted data for the transaction (Fig. 3).

Matsumoto discloses the trustworthy server performing secret computations; decryption is a secret computation.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the trustworthy server and delegate the encryption and decryption calculations to a separate server as in Matsumoto in the broker and server system of Jardin. One of ordinary skill in the art would have been motivated to do this because the system is a trusted network wherein the computing power of an auxiliary device may be implemented.

In reference to claims 3, 21, 40, Jardin discloses a system wherein the packets from the client are encrypted to provide encrypted data for transmission (Fig. 3).

Matsumoto discloses the trustworthy server performing secret computations; encryption is a secret computation.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the trustworthy server and delegate the encryption and decryption calculations to a separate server as in Matsumoto in the broker and server system of Jardin. One of ordinary skill in the art would have been motivated to do this because the system is a trusted network wherein the computing power of an auxiliary device may be implemented.

In reference to claims 4, 22, and 41, Jardin discloses a system wherein the establishing step includes handing off a network connection from the transaction server to the handshake engine such that the handshake engine can establish the cryptographic parameters with a client coupled to the network (Fig. 3 parts 340, 342, 344, 346).

In reference to claims 5, 23, and 42, Jardin discloses a system wherein the servicing step includes handing off a network connection from the handshake engine to the transaction server (column 6 lines 38-55).

In reference to claims 6, 24, and 43, Jardin discloses a system wherein the establishing step includes performing a Secure Sockets Layer (SSL) handshake procedure (column 6 lines 45-47).

In reference to claims 7, 25, and 44, Jardin discloses a system wherein the establishing step includes performing a Transport Layer Security handshake procedure (column 6 lines 45-47 in combination with column 7 lines 40-55). The SSL handshake procedure is performed at the Transport layer.

In reference to claims 8-11, 26-29, 37, 45-48, 54, wherein the transaction is returning at least one of a data file and streaming data. Jardin discloses executing the client transaction and sending a response (column 8 lines 1-10). Data files, streaming data, audio and video data, hypertext, structured data files, and data taken from a form are all sent in the form of packets and therefore are included in the form of data that is disclosed by Jardin.

In reference to claims 12, 30, 49, Jardin discloses a system wherein the cryptographic parameters include at least one cryptographic key (column 5 lines 30-65).

In reference to claims 13, 31, 50, Jardin discloses a system wherein the at least one cryptographic key includes at least one of a public key and a private key (column 5 lines 45-50).

In reference to claims 14, 32, 51, further comprising: notifying the inline crypto engine of the cryptographic parameters.

Jardin does not expressly disclose sending the cryptographic parameters to an auxiliary device that is specifically used for encryption.

However Matsumoto discloses sending the cryptographic parameters, secrets, to a trustworthy server (page 497 Introduction paragraph 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a trusted server as disclosed by Matsumoto and send the cryptographic parameters to the server to perform encryption as in the system taught by Matsumoto to perform the encryption and decryption disclosed by the system of Jardin. One of ordinary skill in the art would have been motivated to do this because the system would use the computational power of the auxiliary device.

In reference to claims 15, 33, 52, Jardin discloses a system receiving a request to establish the cryptographic parameters; and responsive to receiving the request, performing the establishing step (Fig. 2).

In reference to claims 16 and 34, Jardin discloses a system further comprising: receiving the transmitted data from the network by the inline crypto engine (part 430 Fig. 4).

In reference to claims 17 and 35, Jardin discloses a system further comprising: transmitting the transmitted data to the network by the inline crypto engine (part 338 Fig. 3).

In reference to claims 18, 36, and 53, Jardin discloses a system wherein the unencrypted data is a request to perform the transaction (parts 430-434 Fig. 4).

In reference to claim 55, wherein the at least one transaction server, the at least one inline handshake engine, and the at least one inline crypto engine operate concurrently.

Jardin discloses a system with the transaction server and the crypto engine (Fig. 1). Although Jardin does not expressly disclose them operating concurrently, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to operate the inline crypto engine and the inline handshake engine concurrently. One of ordinary skill in the art would have been motivated to do this because the servers are separate, each with its own processor and therefore do not require scheduling to use a shared processor for computation.

In reference to claim 56, wherein the at least one transaction server, the at least one inline handshake engine, and the at least one inline crypto engine operate asynchronously.

Jardin discloses a system with the transaction server, handshake engine, and the crypto engine (Fig. 1). Although Jardin does not expressly disclose the devices operating asynchronously, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to operate the inline crypto engine and the inline handshake engine concurrently. One of ordinary skill in the art would have been motivated to do this because the servers are separate, each with its own processor and therefore do not require scheduling to use a shared processor for computation.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Tuesday, May 31, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100